# NORTH DAKOTA

# HOMELAND SECURITY

# ANIT-TERRORISM SUMMARY

**The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.**

## NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

## QUICK LINKS

## North Dakota

**Corps approves $11.7 million for Williston levee.** The U.S. Army Corps of Engineers awarded $11.7 million in federal funding April 20 to repair and upgrade the levee that separates Williston, North Dakota, and the Missouri River. After heavy rains and record snowmelt in 2011, the levee was damaged as the Missouri reached a record flood stage. No major damage was reported in Williston, however, some lowing structures, roads, and oil wells flooded. “The project was designed to provide protection to the low lying areas of the city against backwater effects from Lake Sakakawea, the reservoir for Garrison Dam,” according to a press release from the Corps. A portion of the money will go to restore the levee crest to an approximate elevation of 1,863 feet above sea level, and the levee will be seeded for grass. Source: http://www.willistonherald.com/news/corps-approves-million-for-williston-levee/article_572b9408-8d6b-11e1-aa28-0019bb2963f4.html

## Regional

(Minnesota) **Humphrey terminal reopened after suspicious package scare.** The Hubert H. Humphrey terminal at the Minneapolis-St. Paul International Airport was cleared and reopened after a suspicious bag was found during pre-screening early April 27. A Metropolitan Airports Commission spokesperson said the suspicious bag set off an alarm during security pre-screening. Airport security could not resolve the situation so a decision was made to call in the Bloomington Police Bomb Squad. Passengers who were already inside the pre-screening area were allowed to stay in the terminal, but anyone that arrived after the discovery of the package was diverted to the parking ramp across the street from the Humphrey terminal. Almost 2 hours later, the bomb squad secured the bag and removed it from the terminal. The owner of the suspicious bag was detained for questioning. Metro Transit reported the activity did not affect light rail service to the airport. Source: http://www.kare11.com/news/article/974617/391/Humphrey-terminal-reopened-after-suspicious-package-scare?odyssey=tab|topnews|bc|large

(Minnesota) **Special delivery May 6 in Twin Cities will test terror attack plan.** Nearly 40,000 Minnesota residents will go to their mailboxes May 6 to find an unusual delivery: an empty pill bottle representing a powerful antibiotic that would be delivered in the event of a bioterrorism attack. The exercise united the Minnesota Department of Health with the U.S. Postal Service. More than 300 mail carriers will participate in the test, fanning out across 4 neighborhoods in Minneapolis, St. Paul, Robbinsdale, and Golden Valley. They plan to reach 37,000 households in 4 ZIP codes. The overall goal would be to deliver preventive doses of medication to most people within the first 48 hours of a bioterror attack. The exercise will spark an intense period of evaluation, when health officials will see if the idea could work under the most catastrophic public health conditions. The tactic has been tested in Boston, Philadelphia, and Seattle, but the Minnesota experiment will be its first full-scale test. A Postal Service spokesman said employee volunteers had to go through hours of safety training and preparation for the exercise — including being fitted with protective masks. Local law enforcement officials will escort postal workers, as they would be in a true emergency. The biggest logistical concern for the health department and Postal Service has been informing the participating communities. Source: http://www.startribune.com/lifestyle/health/148607855.html

## National

**Winter returns with a blast as snow pounds U.S. Northeast.** A snowstorm struck a wide area of the Northeast April 23, raising the threat of downed trees and hazardous roads and causing scattered power outages in several states. The National Weather Service issued winter storm warnings from West Virginia northward into western New York. As much as a foot of snow was forecast for higher elevations of western Pennsylvania. About 57,000 power outages were reported scattered across several states from Kentucky to Maine, with most of them in Pennsylvania and upstate New York. Portions of southern New England continued to receive soaking rain as strong winds picked up along the coast, prompting a flood advisory for the area. Winds of up to 50 miles per hour were expected in some areas, the service said on its Web site. Source: http://www.orlandosentinel.com/news/nationworld/sns-rt-us-usa-weather-northeastbre83l08z-20120422,0,7491536.story

## International

**U.S. warns of terror attack targeting hotels in Kenya.** The U.S. Embassy in Nairobi, Kenya, warned April 23 it received "credible information" regarding an attack on hotels and government buildings in the Kenyan capital. "Timing of the attack is not known, however, the Embassy has reason to believe that the potential attack is in the last stages of planning. The U.S. Embassy urges Americans to remain aware of their surroundings and vigilant of their personal security," the message posted on the embassy's Web site stated. The message provided no further details on the nature of the threat. Source: http://www.foxnews.com/world/2012/04/23/us-warns-terror-attack-targeting-hotels-in-kenya/

**Audit confirms EPA radiation monitors broken during Fukushima crisis.** An internal audit confirmed observers' concerns that many of the U.S. Environmental Protection Agency's (EPA) radiation monitors were out of service at the height of the 2011 Fukushima power plant meltdown in Japan, Government Security Newswire reported April 23. The report detailed problems with the agency's "RadNet" monitoring system. Agency contractors are responsible for maintaining the monitors and repairing them when they are broken. However, according to the report, the EPA has not managed those contracts as high priorities, despite having identified the monitors as "critical infrastructure" under the 2001 Patriot Act. As a result, there have been numerous delays in repairing broken monitors. In addition, the agency has in many instances allowed filters to go unchanged for longer than the twice-per week that its policy dictates, the audit said. Because of these issues, 20 percent of the monitors were out of service the day the Fukushima crisis began, according to the report. Source: http://www.nti.org/gsn/article/audit-confirms-epa-radiation-monitors-broken-during-fukushima-crisis/

**Italy police seize $5 billion of U.S. securities.** Italy financial police have seized U.S. securities with face values of about $1.5 billion and gold certificates worth above $3.96 billion as part of an investigation into a possible international financial scam. The police said April 21 the "million dollar" operation was a last step in the probe, which centered on the use of bearer Federal Reserve debt securities dating back to the 1930s as a guarantee for loans or other opaque cross-border transactions. Rome police seized the securities from a man, who held them in a briefcase along with documents about financial operations, the police said in a statement. Police said they were carrying out checks, helped by the U.S. Central Bank and the U.S. embassy in Rome, over the authenticity and origin of the securities, as well as over possible links between the man and criminal organizations. Source: http://www.reuters.com/article/2012/04/21/us-italy-police-seize-idUSBRE83K08F20120421

## Banking and Finance Industry

**NYSE receives credible cyber threat against website.** The New York Stock Exchange (NYSE) received a credible threat to disrupt its external Web site as part of an apparent cyber attack attempt against many U.S. exchanges, the Fox Business Network reported April 26. The threat, which is not tied to NYSE's trading systems, prompted the Big Board to beef up security and monitoring for a potential cyber attack, sources familiar with the matter said. The April 26 threats centered around a potential denial-of-service attack strictly focused on the exchange's external Web site, and having nothing to with its trading systems, a source said. The cyber threat appears to be tied to an anti-capitalistic online posting by a cyber group called "L0NGwave99" that promised to hit stock exchanges with a denial of service attack April 26 in support of the "great and rooted 99% movement." In addition to the NYSE, the group claimed it will put "into a profound sleep" the Web sites of the Nasdaq Stock Exchange, BATS, the Chicago Board of Options Exchange, and the Miami Stock Exchange. While the posting said it would start the operation at 9 a.m., none of those exchanges appeared to be suffering any Web site difficulties as of early the afternoon of April 26. Source: http://www.foxbusiness.com/industries/2012/04/26/nyse-receives-credible-cyber-threat/

**Credit card 'info for sale' websites closed in global raids.** Dozens of Web sites offering credit card details and other private information for sale have been taken down in a global police operation, BBC News reported April 26. Britain's Serious Organized Crime Agency (SOCA) said the raids in Australia, Europe, the United Kingdom, and the United States were the culmination of 2 years of work. Two Britons and a man from Macedonia were arrested, with 36 sites shut down. Some of the Web sites have been under observation for 2 years. During that period the details of about 2.5 million credit cards were recovered — preventing fraud, according to industry calculations, of about $809 million. The head of SOCA's cyber crime unit said criminals were selling personal data on an "industrial" scale. He said traditional "bedroom" hackers were being recruited by criminal gangs to write the malware or "phishing" software that steals personal data. Other information technology experts are used to write the code that enables the Web sites to cope, automatically, with selling the huge amounts of data. Joint operations April 26 in Australia, the United States, Britain, Germany, the Netherlands, Ukraine, Romania, and Macedonia led to the Web sites being closed down. Source: http://www.bbc.co.uk/news/uk-17851257

**Bank of America phishing emails doing rounds.** Fake warning e-mails are targeting Bank of America customers and asking them to update their account. With "Bank of America Warning : Error Statement" in the subject line, the vaguely credible HTML e-mail states the target's "Bank of America account showed unusual activities this morning." "What to do next? Sign in now to verify your logon details," the e-mail urges. Unfortunately, all the links in the e-mail take the recipient to a spoofed Bank of America Web site, where they are asked to sign in by entering their log-in details and are prompted to share additional personal and financial information to "verify" their accounts. "The care and detail with which the scam email has been created makes this phishing scam attempt a little more sophisticated than some other such attacks and may fool at least a few bank customers into supplying the requested details," according to Hoax-Slayer. Source: http://www.net-security.org/secworld.php?id=12788

**Russian cybercriminals earned $4.5 billion in 2011.** Russian-speaking hackers earned an estimated $4.5 billion globally using various online criminal tactics and are thus responsible for 36 percent of the estimated total of $12.5 billion earned by cybercriminals in 2011, Russian security analyst firm Group-IB said in a report published April 24. The researchers estimate the total share of the Russian cybercrime market alone doubled to $2.3 billion, while the whole Russian-speaking segment of the global cybercrime market almost doubled, to $4.5 billion. In 2011, the cybercrime market was embraced by traditional organized crime groups trying to control the entire theft process. The cybercrime market has consolidated, with the rise of several major groups. This could lead to "an explosive increase of attacks" on the financial sector, the researchers warned. Online banking fraud, phishing attacks, and the theft of stolen funds increased within Russia and was the largest area of cybercrime, amounting to an estimated $942 million. In Russia, there also was a trend in targeting individuals rather than financial institutions for online banking fraud, and criminals mainly used Web-inject technologies and trojan programs to lead users to phishing sites. Source: http://www.computerworld.com/s/article/9226498/Russian_cybercriminals_earned_4.5_billion_in_2011

**Phishing and malware meet check fraud.** Trusteer recently uncovered a scam in an underground forum that shows how data obtained through phishing and malware attacks can be used to make one of the oldest forms of fraud — check forging — even harder to prevent. The scam involves a criminal selling pre-printed checks linked to corporate bank accounts in the United States, the United Kingdom, and China. The criminal is selling falsified bank checks made with specialized printing equipment, ink, and paper. For $5 each, they will supply checks that use stolen data provided by the buyer. However, to purchase checks that use stolen credentials supplied by the counterfeiter the cost is $50. Check data fields include personal information and financial data. To obtain all the required data, fraudsters typically must get their hands on a physical or scanned version of a real check in circulation. Many banking Web sites provide access to scanned versions of paid and received checks. Online banking log-in credentials obtained through malware and phishing attacks can be used to access a victim's account and collect all the required information to commit check fraud. Also, before using the checks, fraudsters can ensure account balance is sufficient to approve the transaction. The criminal recommends using the checks to buy products in stores rather than trying to redeem them for cash. Buyers are encouraged to carry fake identification cards that match stolen credentials on the check. The check counterfeiter offers to provide these too. Source: http://www.net-security.org/secworld.php?id=12793

**FinCEN reports mortgage fraud SARs increased in 2011 even as fourth quarter level decreased.** The Financial Crimes Enforcement Network (FinCEN) April 23 released its full year 2011 update of mortgage loan fraud reported suspicious activity reports (MLF SARs) that showed financial institutions submitted 92,028 MLF SARs in 2011, a 31 percent increase over the 70,472 submitted in 2010. The increase can primarily be attributable to mortgage repurchase demands. Financial institutions submitted 17,050 MLF SARs in the 2011 fourth quarter, a 9 percent decrease in filings over the same period in 2010 when financial institutions filed 18,759 MLF SARs. The fourth quarter of 2011 was the first time since the fourth quarter of 2010 when filings of MLF SARs had fallen from the previous year. FinCEN also updated its SAR data sets used in the report. Source: http://www.fincen.gov/news_room/nr/html/20120423.html

## Chemical and Hazardous Materials Sector

**MSHA to phase out potentially faulty breathing devices.** Federal mine safety officials have ordered immediate phase-out of a self-contained self-rescue device (SCSR) found to have potential for failure, the Charleston State Journal reported April 26. The breathing devices were found to have a "low-probability" of failure, so the agency ordered the SCSR devices from Pittsburgh-based CSE corp. to be removed from the nation's mines. The Mine Safety and Health Administration (MSHA) made the announcement April 26. "Due to the large number of CSE SR-100s in underground coal mines, multiple SCSRs available to miners, the low probability of failure and the shortage of immediately available replacements, MSHA and [the National Institute for Occupational Safety and Health (NIOSH)] have determined an orderly phase-out will better protect the safety of miners than immediate withdrawal of the devices," said the assistant secretary of labor for mine safety and health. The rescue devices are designed to provide underground coal miners with up to 60 minutes of breathable air in the event of an emergency. A joint investigation by the NIOSH and the MSHA found the units did not conform to safety requirements. Source: http://www.statejournal.com/story/17795242/msha-to-phase-out-potentially-faulty-breathing-devices

**New U.S. rules against harmful chemicals in dyes.** The U.S. Environmental Protection Agency (EPA) has asked all U.S.-based clothing and apparel manufacturers to report the new use of possibly harmful chemicals found in textile pigments and dyes, just-style.com reported April 25. The chemicals, which also have other industrial applications, include polybrominated diphenylethers, benzidine dyes, and hexabromocyclododecane. "Although a number of these chemicals are no longer manufactured or used in the United States, they can still be imported in consumer goods or for use in products," an EPA spokesman said. The new rules are outlined under the Toxic Substances Control Act. They require any person or company to notify the EPA

90 days before they manufacture, import, or process any of the chemicals specified, so the EPA can evaluate the chemicals and decide if they are safe. If the action is warranted, the EPA retains the right to prohibit certain new uses of the named chemicals. Source: http://www.just-style.com/news/new-rules-against-harmful-chemicals-found-in-dyes_id114159.aspx

## Commercial Facilities

Nothing Significant to Report

## Communications Sector

**Engineers look to fix Internet routing weakness.** Information technology engineers are studying what may be an easier way to fix a long-existing weakness in the Internet's routing system that has the potential to cause major service outages and allow hackers to spy on data, IDG News Service reported April 26. The problem involves the routers used by every organization and company that owns a block of Internet Protocol (IP) addresses. Those routers communicate constantly with other routers, updating internal information — often upwards of 400,000 entries — on the best way to reach other networks using a protocol called Border Gateway Protocol (BGP). Changes in that routing information are distributed quickly to routers around the world in as few as 5 minutes. But the routers do not verify the route "announcements," as they are called, are correct. Mistakes in entering the information — or a malicious attack — can cause a network to become unavailable. It can also cause, for example, a firm's Internet traffic to be circuitously routed through another network it does not need to go through, opening the possibility the traffic could be intercepted. The attack is known as "route hijacking," and cannot be stopped by any security product. The solution is to have routers verify the IP address blocks announced by others' routers actually belong to their networks. Source: http://www.computerworld.com/s/article/9226657/Engineers_look_to_fix_Internet_routing_weakness?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google+Read

**FCC adds VoIP and broadband providers to its disaster reporting system.** The U.S. Federal Communications Commission (FCC), which has already established a Disaster Information Reporting System (DIRS) to gather contact information from wireless, wireline, broadcast, cable, and satellite communications providers that might be useful during an emergency, has decided to expand the coverage of the DIRS to include Voice over Internet Protocol (VoIP), Internet Protocol, and broadband Internet Service Providers. The FCC decided to take this step because so many consumers, businesses, and government agencies have come to rely on broadband and VoIP services for their everyday and emergency communications, according to a Federal Register notice posted by the FCC April 23. Source: http://www.gsnmagazine.com/node/26174?c=communications

(Vermont) **Thieves steal live telephone lines.** Police said someone cut down several telephone lines in Dover, Vermont, to steal the copper. According to the Dover police chief, at about 3 a.m. April 20 about 800 feet of cable was cut from the utility poles along North Street in the East Dover section of town. Police were first alerted to the theft after FairPoint Communications said they had received a report of an outage and discovered the missing telephone lines at the scene. The chief said he is looking into the possibility of bringing in the FBI to assist with the case. Source: http://www.reformer.com/localnews/ci_20473719/thieves-steal-live-telephone-lines

**Plumbers of the interwebs vow to kill IP hijacking.** The Internet Engineering Task Force (IETF) aims to strengthen the basic protocols of the Internet, with a way to stop route, or IP, hijacking, The Register reported April 23. IETF experts say the proposed fix is simpler to implement than previous suggestions. IP hijacking exploits a fundamental weakness of the Internet — data and messages sent across the Internet are transmitted via routers, and those routers are blindly trusted. No measures are in place to verify if they have been tampered with to re-direct or intercept traffic. At an IETF meeting in March, a working group proposed a solution that seeks to safeguard the integrity of networking kit. The proposal involves publishing preferred routes to sites in DNS records before applying a second step, using utilities to verify the instructions are trustworthy. This latter step would use DNS Security Extensions, a separate security mechanism being rolled out as a defense against cache-poisoning attacks. The whole scheme is called ROVER, or BGP Route Origin Verification (via DNS). Rover calls for the use of reverse DNS records to periodically publish route announcements, a process that would be done by sites themselves, before carrying out real-time verifications of BGP route announcements. Rover uses “best effort” data retrieval with worldwide data distribution, redundancy, and local caching. If the data is unreachable, the default is that routing would proceed as normal but without any checks. Source: http://www.theregister.co.uk/2012/04/23/ip_hijack_prevention/

## Critical Manufacturing

**Nissan gets hacked, target could’ve been intellectual property.** Nissan Motor Company announced that its information systems were hacked, Daily Tech reported April 24. The company did not know who the hackers were or where they struck from, and it was unclear what data may have been compromised. Nissan believes the hackers were looking for intellectual property related to its EV drivetrains. Nissan maintained it quickly secured its system and issued a statement alerting customers and employees that its data systems were breached. Nissan said the infiltration was noticed April 13. A Nissan statement said the company’s security team confirmed the presence of a computer virus on their network, and took action to protect systems and data. Source: http://www.dailytech.com/Nissan+Gets+Hacked+Target+Couldve+Been+Intellectual+Property/article24527.htm

**Gem Sensors recalls pressure transducers used in fire pump controllers due to risk of failure in a fire.** The U.S. Consumer Product Safety Commission, in cooperation with Gems Sensors, April 24 announced a voluntary recall of about 25,000 Gems 3100 pressure detectors/transducers. The transducer can fail to accurately detect water pressure in a fire suppression sprinkler system. This could cause the sprinkler system to fail to activate and pump water to the sprinklers in the event of a fire. Owners were advised to contact Gems to receive enhanced twice monthly inspection instructions and information about a free replacement transducer, when warranted. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12156.html

## Defense/ Industry Base Sector

**Miscoordination slows U.S. missile defense preparations: GAO.** The U.S. Defense Department's strategy of simultaneously pursuing multiple preparatory phases for its missile defense systems has resulted in unnecessary delays of certain equipment, the Government Accountability Office (GAO) said in a report issued April 25. Drawing from previous GAO findings, congressional auditors found such parallel operations to exist at "high levels" in policies the Pentagon's Missile Defense Agency adopted previously and in the present to obtain antimissile systems. The antimissile office has pursued many reforms, but "considerable risk" would persist for "future performance shortfalls that will require retrofits, cost overruns, and schedule delays" if the Pentagon pursues such simultaneous preparations for antimissile efforts at later dates, the report warns. The Pentagon endorsed six of seven guidelines provided by Congressional investigators for curbing such practices and "partially agreed" with the remaining advisory statement. Separately, the Missile Defense Agency is taking many steps in response to concerns voiced by GAO auditors in June 2011 over possible problems with antimissile components, the document states. The measures involved "internal policies, collaborative initiatives with other agencies, and contracting strategies to hold its contractors more accountable," investigators wrote. Source: http://www.nti.org/gsn/article/miscoordination-slows-us-antimissile-preparations-gao/

## Emergency Services

(Maine) **Emergency radios jammed in York County.** Maine's Lebanon Rescue Department is offering a $500 reward for information leading to the person who has been jamming their radios. The assistant chief said other departments have been affected too. He said the person sometimes blocks out radio traffic, or sometimes whistles into the radio, making it impossible for emergency crews to get their calls out. The interference has become more and more frequent, and the assistant chief said April 22 it went to a new level when the person actually blocked him from radioing for advanced life support for a patient. Lebanon rescue is now working with the Federal Communications Commission to see if the person's radio signal can be traced. Source: http://www.wlbz2.com/news/article/198838/3/Emergency-radios-jammed-in-York-County

(Hawaii) **Man posing as FBI agent on Maui arrested.** Maui, Hawaii police said officers arrested a man in Kahului April 16 for theft, forgery, and impersonating a law enforcement officer. He is accused of impersonating an FBI agent to a Maui family. He asked the family to go into their home and investigate a "cyber" crime that involved their daughter and a Facebook account.

The victims gave him the key to their home and, upon returning home, they noticed missing items that totaled $1,630; Bank of Hawaii records also show the man tried to cash a personal check from the victims in the total amount of $1,000. When police arrested him, they found a .38 caliber revolver, a TASER, three air soft handguns, two air soft rifles with scopes, two FBI badges, one Maui police badge, a hand grenade, ammunition, gunpowder, and FBI and police raid clothing in his home. The FBI was notified and responded. The FBI planned to pursue federal charges against the man. Source: http://www.kitv.com/news/hawaii/Man-posing-as-FBI-agent-on-Maui-arrested/-/8905354/11311284/-/h7td00z/-/

## Energy

**Safe fracking require distance from sensitive rock strata.** The chances of rogue fractures due to shale gas fracking operations extending beyond 0.6 kilometers from the injection source is a fraction of 1 percent, according to new research led by Durham University, Homeland Security NewsWire reported April 26. The analysis is based on data from thousands of fracking operations in the United States and natural rock fractures in Europe and Africa. It is believed to be the first analysis of its type and could be used across the world as a starting point for setting a minimum distance between the depth of fracking and shallower aquifers used for drinking water. The new study, published in the journal Marine and Petroleum Geology, shows the probabilities of "rogue" fractures, induced in fracking operations for shale gas extraction, extending beyond 0.6 kilometers from the injection source are exceptionally low. The probability of fractures extending beyond 350 meters was found to be 1 percent. During fracking operations, fractures are created by drilling and injecting fluid into the rock strata underground to increase oil and gas production from fine-grained, low permeability rocks, such as shale. These stimulated fractures can significantly increase the rate of production of oil and gas from such rocks. Of the thousands artificially induced, none were found to exceed 600 meters, with the vast majority being much less than 250 meters in vertical extent. Source: http://www.homelandsecuritynewswire.com/dr20120426-safe-fracking-requires-distance-from-sensitive-rock-strata

**Smart-grid tech outpacing security, in ‘delicate dance with risk’.** Development and deployment of smart-grid technology such as intelligent electric meters has outpaced security, setting up a “delicate dance with risk,” according to the head of an industry advisory group, Government Computer News reported April 23. The head of the Energy Sector Security Consortium (EnergySec), a non-profit forum for the exchange of security information among asset owners, industry partners, and the U.S. government, said installation of new equipment is already under way and slowing down to wait for security to catch up is not an option. He made his comments in the wake of a survey of energy industry security professionals in which large majorities of respondents said that security controls and standards are not keeping pace with the rollout of new equipment. Source: http://gcn.com/articles/2012/04/23/smart-grid-tech-outpaces-security-hacker-opportunity.aspx

## Food and Agriculture

**Search underway for any more 'mad cows'.** The dead Hanford, California dairy cow with laboratory-confirmed bovine spongiform encephalopathy (BSE) is now the centerpiece of an investigation into whether there are any more mad cows in the vicinity, Food Safety News reported April 26. Dairymen in the Central Valley of California were told that state and federal officials are testing the BSE-infected animal's feeding herd, which could include some of its own offspring, and other cows in the area born about the same time. Baker Commodities, the Los Angeles-based company that owns the transfer rendering station at Hanford, also announced it was holding the diseased carcass in cold storage, as well as all other cows that arrived with it on the same truck. It was Baker's participation in a random sampling program that returned the BSE-infected brain tissue, 1 of 40,000 samples the U.S. Department of Agriculture plans to take in 2012. The BSE-infected carcass was in quarantine where it will remain until state and federal officials order it destroyed. The exact location of the dairy farm where the diseased cow lived and died on or before April 18 has not been disclosed. The Hanford dairy cow did not show any "mad cow" signs — such as difficulty walking — before it died, making investigators especially interested in testing its calves and cohorts. Source: http://www.foodsafetynews.com/2012/04/search-begins-for-other-mad-cows-in-central-valley/

**Pathogen test rapidly hones in on Salmonella.** A new method of testing for Salmonella could shorten the time it takes to detect the bacteria in food samples, Food Safety News reported April 23. Researchers at the Agricultural Research Service’s Quality and Safety Assessment Unit in Athens, Georgia, are using a technique called surface-enhanced Raman scattering (SERS), in which light from a laser is directed at a sample specimen, whose interaction with the light produces a unique spectral pattern called a “Raman spectral signature.” Scientists postulate that each strain of bacteria has its own unique signature that acts as a badge of identity. Currently, bacteria are most often identified by their DNA fingerprint using pulsed-field gel electrophoresis (PFGE). These PFGE patterns are then uploaded onto PulseNet, a national database that can be used to see if the strain matches others in the system. However, PFGE analysis usually takes at least 24 hours to complete in a lab, whereas a test using SERS takes less than 30 minutes from start to finish, according to the lead researcher. He said if SERS proves effective, a worldwide Internet database could be created using Raman spectral signatures to find a match for bacteria more quickly, which could help investigators pinpoint the source of contamination earlier in an outbreak. Source: http://www.foodsafetynews.com/2012/04/pathogen-test-rapidly-hones-in-on-salmonella/

**USDA tightens rules for drug residues in food animals.** Federal meat safety officials are stepping up efforts to prevent meat with illegal levels of drugs or other chemicals from entering the food supply. The new plan — unveiled April 23 by the U.S. Department of Agriculture’s Food Safety and Inspection Service (FSIS) — is two-pronged. First, the agency will release a new compliance guide for slaughter establishments outlining measures that can reduce or prevent residues in livestock. FSIS will also increase residue testing at establishments with a record of residue violations, the agency said. This will protect meat containing residues from entering the food supply, and also will give past violators an incentive to use methods that do not produce illegal residue amounts. If cows were administered antibiotics, anti-inflammatory medicines, or other drugs, different withdrawal times, depending on the drugs, must elapse before they may be slaughtered and marketed. Culled cows that contain drug residues are not supposed to be sold to slaughterhouses nor is meat from animals with drug residues to be shipped into commerce. The new guidance is intended especially for establishments that slaughter dairy cows or bob veal calves, since these operations commit the majority of residue violations. FSIS also announced it is revamping its Residue Repeat Violator List — maintained by the National Residue Program — to make it "streamlined and more user-friendly." Source: http://www.foodsafetynews.com/2012/04/usda-strengthens-prevention-of-residues-in-food-animals/

**S. Korea curbs U.S. beef sales after confirmation of mad cow disease.** At least one major South Korean retailer suspended the sale of U.S. beef after authorities confirmed a case of bovine spongiform encephalopathy (BSE), sometimes called "mad cow disease," in a dairy cow in central California, CNN reported April 25. Public health officials in the United States said the risk to the public was extremely low, and residents do not need to take any specific precautions. However, in South Korea, one of the largest importers of U.S. beef, the discovery was enough to prompt retailer LotteMart to remove American beef from store shelves. The South Korean government said it will step up checks on U.S. beef imports — but not halt them for now. In 2010, South Korea imported 125,000 tons of U.S. beef, a 97 percent increase from the year before, the U.S. Department of Agriculture said. The carcass was at a Baker Commodities Inc. rendering facility in Hanford, California, said the company's executive vice president. The company renders animal byproducts and had randomly selected the animal for testing April 18, he said. The sample was sent to the University of California, Davis for initial testing, which came back inconclusive. It was then sent to the U.S. Department of Agriculture's laboratory in Ames, Iowa, where it tested positive, the agency said. The carcass was in quarantine April 24. BSE is usually transmitted between cows through the practice of recycling bovine carcasses for meat and bone meal protein, which is fed to other cattle. In this case, the USDA reports it was a rare form of BSE not likely carried by contaminated feed. The Centers for Disease Control and Prevention reported the odds of a person contracting mad cow disease, even after consuming contaminated products, are less than 1 in 10 billion. Source: http://www.cnn.com/2012/04/25/health/california-mad-cow/index.html

**Sushi salmonella outbreak total rises to 160 confirmed cases.** Nineteen more cases of Salmonella Bareilly infection were confirmed in the multistate outbreak linked to sushi tuna. At least 160 people in 20 states and Washington, D.C. have been sickened, the Centers for Disease Control and Prevention (CDC) reported April 20. The CDC said the outbreak is likely much larger, estimating that for every case of salmonellosis, 38.6 go unreported. That would translate to about 6,176 people ill from eating tainted tuna. The implicated frozen raw yellowfin tuna product was imported from India and was recalled by the California-based distributor, Moon Marine USA. According to the CDC's latest update, the 19 new outbreak cases include 14 reported by Massachusetts, 2 reported by New York, and 1 each reported by Illinois, North Carolina, and Virginia. The ill people range in age from 4 to 78 years, and 66 percent are female.

At least 26 have been hospitalized. Source: http://www.foodsafetynews.com/2012/04/sushi-salmonella-outbreak-total-rises-to-160-cases/

(Oregon) **19 ill with E. coli in Oregon raw milk outbreak.** Another person in Oregon became ill after an E. coli outbreak was traced to raw milk from Foundation Farm near Wilsonville, according to a April 20 news release from the public health division of the state's health authority. Of the 19 total cases, 11 have culture-confirmed E. coli O157 infections. Fifteen of the cases are children 19 or younger, four of the children were hospitalized with kidney failure. According to a member of the cowshare implicated in the outbreak, as many as four of the farmer's children are also sickened, including one with hemolytic uremic syndrome. Source: http://www.foodsafetynews.com/2012/04/post-5/

## GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

**UGNazi hackers launch DDOS attacks on CIA, DOJ sites to protest CISPA.** Hackers from the UGNazi group launched attacks on the sites of the CIA and the Department of Justice (DOJ) April 24 to show they do not agree with a new anti-piracy law, the Cyber Intelligence Sharing and Protection Act (CISPA). While the site of the DOJ seemed to be restored, the one of the CIA was down for at least 8 hours. Starting the weekend of April 21, members of the UGNazi group were attacking sites that belong to the U.S. government and organizations they consider corrupt. Their first targets were the Web sites of New York City and the Government of the District of Columbia, which they considered to be "the heart" of the United States. Then they moved to NASDAQ, whose public facing Web site they kept down for a few hours. The State of Washington site was attacked April 21, being kept offline for more than 4 hours. Source: http://news.softpedia.com/news/UGNazi-Hackers-Launch-DDOS-Attack-on-CIA-DOJ-Site-to-Protest-CISPA-266033.shtml

**Cyberattacks on U.S. federal IT system soared 680% in five years.** Cyberattacks on the federal government's IT systems skyrocketed 680 percent in 5 years, an official from the Government Accountability Office (GAO) testified the week of April 23 on Capitol Hill. Federal agencies reported 42,887 cybersecurity incidents in 2011, compared with just 5,503 in 2006, the director of information issues for the GAO told a House Homeland Security Committee panel. The incidents reported by the agencies included unauthorized access to systems, improper use of computing resources, and the installation of malicious software, among others. The GAO official said the sources of the cyberthreats included criminal groups, hackers, terrorists, organizational insiders, and foreign nations. "The magnitude of the threat is compounded by the ever-increasing sophistication of cyber attack techniques, such as attacks that may combine multiple techniques. Using these techniques, threat actors may target individuals, businesses, critical infrastructures, or government organizations," he testified. The federal government's IT systems continue to suffer from "significant weaknesses" in information security controls, he said. Eighteen of 24 major federal agencies have reported inadequate information security controls for financial reporting for fiscal year 2011, and inspectors general at 22 of these agencies identified information security as a major management challenge for their agency, he told the House panel. ”Reported attacks and unintentional incidents involving federal, private, and infrastructure systems demonstrate that the impact of a serious attack could be significant, including loss of personal or sensitive information, disruption or destruction of critical infrastructure, and damage to national and economic security,” he warned. Source: http://www.infosecurity-magazine.com/view/25393/cyberattacks-on-us-federal-it-system-soared-680-in-five-years/

**Hackers targeting governments with hijacked sites.** Malicious code planted within compromised Wed pages has become the latest method for attackers targeting government organizations, according to research from security firm Zscaler, V3.co.uk reported April 21. The firm discovered many government-affiliated Web sites with code that directs users to attack servers. The most recent site to become infected was that of the French budget minister. It was found to contain obfuscated Javascript code that sends the user to a third party site and then attempts to exploit vulnerabilities and install malware on the targeted system. The attack is the latest in what Zscaler sees as a string of site hijackings aimed at government-controlled domains. Researchers noted previous attacks on systems in the United States, Austria, and Malaysia. Zscaler’s chief executive believes the attacks are the work of state-sponsored operations aimed at infecting government workers and other high-value targets. A Zscaler security researcher said organizations often leave a few of their less popular sites and portals poorly maintained and protected, leaving a back door open for attackers. Source: http://www.v3.co.uk/v3-uk/news/2169452/hackers-targeting-governments-hijacked-sites

(Missouri) **Explosive device thrown at federal building in downtown St. Louis.** Federal officials are investigating after someone threw an explosive device at the Robert A. Young federal building in downtown St. Louis, Missouri, April 23, authorities said. The building the device was thrown at houses several government agencies, including Homeland Security, Housing and Urban Development, the U.S. Coast Guard, and the U.S. Army Corps of Engineers. According to authorities, the device landed on the sidewalk outside the building and exploded. No injuries were reported and there was very little damage done. According to reports, a witness saw the male suspect who threw the device. The witness pursued the man, but he got into a gray Chevy Camaro with Illinois license plates and took off. The vehicle is described as a 1990’s model with no hubcaps and partial license “N50.” Source: http://www.kmov.com/news/local/Explosive-device-thrown-at-federal-building-in-downtown-St-Louis-148487785.html

## Information Technology and Telecommunications

**One vulnerable site can serve multiple cybercriminal groups, experts find.** Security researchers found that a single vulnerable Web site may be used by a number of cybercriminal organizations, each one altering the site to serve its own purposes. In many cases, Web sites are compromised and altered to lead visitors to domains that push fake antivirus programs, which lately have become a great way for cyber criminals to earn a profit. A Zscaler expert explained that once the criminals overtake the site, they rely on Blackhat SEO techniques to increase traffic towards their malicious plots. In order to do this, they set up two different pages on the compromised domain. First, they create a spam page that search engines, security scanners, and blacklisting mechanisms see as harmless. This page does not contain obfuscated code and performs the redirect via a PHP or .htaccess file. The second page contains the redirect to a site in charge of performing the attack on users. More recently, researchers identified many overtaken Web sites designed to send users to fake antivirus were also infected with a malicious piece of JavaScript, which held an IFRAME injection that pointed to several different locations. Source: http://news.softpedia.com/news/One-Vulnerable-Site-Can-Serve-More-Cybercriminal-Groups-Experts-Find-266737.shtml

**Backdoor in mission-critical hardware threatens power, traffic-control systems.** Equipment running RuggedCom's Rugged Operating System networking gear has an undocumented account that cannot be modified and a password that is trivial to crack. According to researchers, for years the company did not warn the power utilities, military facilities, and municipal traffic departments using the industrial-strength gear the account can give attackers the means to sabotage operations that affect the safety of many people. The backdoor uses the login ID of "factory" and a password recovered by plugging the media access control (MAC) address of the targeted device into a simple Perl script, according to a post published April 23 to the Full Disclosure security list. To make unauthorized access easy, paying customers of the Shodan computer search engine can find the IP numbers of more than 60 networks that use the vulnerable equipment. The first thing users who telnet into them see is its MAC address. Equipment running the Rugged Operating System act as the switches and hubs that connect programmable logic controllers to the computer networks used to send them commands. They may lie between the computer of a electric utility employee and the compact disk-sized controller that breaks a circuit when the employee clicks a button on their screen. To give the equipment added power, Rugged Operating System is fluent in the Modbus and DNP3 communications protocols used to natively administer industrial control and supervisory control and data acquisition systems. The U.S. Navy, the Wisconsin Department of Transportation, and Chevron are just three of the customers who rely on the gear, according to RuggedCom's Web site. Source: http://arstechnica.com/business/news/2012/04/backdoor-in-mission-critical-hardware-threatens-power-traffic-control-systems.ars?utm

**Most of the Internet's top 200,000 HTTPS websites are insecure, group says.** Ninety percent of the Internet's top 200,000 HTTPS-enabled Web sites are vulnerable to known types of secure sockets layer (SSL) attack, according to a report released April 26 by the Trustworthy Internet Movement (TIM), a nonprofit organization dedicated to solving Internet security, privacy, and reliability problems. It is based on data from a new TIM project called SSL Pulse, which uses automated scanning technology developed by security vendor Qualys to analyze the strength of HTTPS implementations on Web sites in the top 1 million published by Web analytics firm Alexa. SSL Pulse checks what protocols are supported by HTTPS-enabled Web sites, the key length used for securing communications, and the strength of the supported ciphers. An algorithm is used to interpret scan results and assign a score between 0 and 100 to each HTTPS configuration. The score is then translated into a grade, with A being the highest (over 80 points). Half of the almost 200,000 Web sites in Alexa's top 1 million that support HTTPS received an A for configuration quality. The sites use a combination of modern protocols, strong ciphers, and long keys. Despite this, only 10 percent of the scanned Web sites were deemed truly secure. Seventy-five percent — around 148,000 — were found to be vulnerable to an attack known as BEAST, which can be used to decrypt authentication tokens and cookies from HTTPS requests. Source: http://www.computerworld.com/s/article/9226623/Most_of_the_Internet_39_s_top_200_000_HTTPS_websites_are_insecure_group_says

**Expert accidentally finds how DoS attacks can be launched via Google.** A computer scientist working at New York University learned Google can be used to launch successful denial-of-service (DoS) attacks against sites with minimal effort. The researcher explained it started when he saw Amazon Web Services was charging him with 10 times the usual amount because of large amounts of outgoing traffic. After analyzing traffic logs, he was able to determine that every hour a total of 250 gigabytes of traffic was sent out because of Google's Feedfetcher, the mechanism that allows the search engine to grab RSS or Atom feeds when users add them to Reader or the main page. It appears Google does not want to store the information on its own servers so it uses Feedfetcher to retrieve it every time, thus generating large amounts of traffic. This enabled the expert to discover how a Google feature can be easily used to launch attacks against a site simply by gathering several big URLs from the target and putting them in a spreadsheet or a feed. If the feed is placed into a Google service or a spreadsheet and the image(url) command is used, a DoS attacks is initiated. Source: http://news.softpedia.com/news/Expert-Accidentally-Finds-How-DOS-Attacks-Can-Be-Launched-Via-Google-266613.shtml

**Anonymous hackers dominate IT security pros' fears.** According to the 2012 Bit9 Cyber Security Research Report, 64 percent of IT security professionals believe their organizations will be targeted by cyberattacks within the next 6 months, and 61 percent say those attacks are most likely to be led by members of Anonymous or other hacktivists. However, the attack methods that dominate security pros' concerns are not tied to Anonymous. Forty-five percent of respondents are most worried about malware attacks, and 17 percent are concerned about spear phishing (both common attack methods for cybercriminals and nation states), while Anonymous' favored method, the distributed denial-of-service attack, leads the concerns of only 11 percent of respondents. Source: http://www.esecurityplanet.com/hackers/anonymous-hackers-dominate-it-security-pros-fears.html

**Anonymous hackers dominate IT security pros' fears.** According to the 2012 Bit9 Cyber Security Research Report, 64 percent of IT security professionals believe their organizations will be targeted by cyberattacks within the next 6 months, and 61 percent say those attacks are most likely to be led by members of Anonymous or other hacktivists. However, the attack methods that dominate security pros' concerns are not tied to Anonymous. Forty-five percent of respondents are most worried about malware attacks, and 17 percent are concerned about spear phishing (both common attack methods for cybercriminals and nation states), while Anonymous' favored method, the distributed denial-of-service attack, leads the concerns of only 11 percent of respondents. Source: http://www.esecurityplanet.com/hackers/anonymous-hackers-dominate-it-security-pros-fears.html

**TreasonSMS bug allows hackers to execute malicious code on iPhones.** Researchers from the Vulnerability Lab found high severity HTML Inject and File Include security holes in TreasonSMS, an iPhone application that allows users to send text messages from their desktop computers by turning the phone into a SMS Web server. According to the experts, the vulnerabilities can be exploited remotely, allowing an attacker to "include malicious persistent script codes on the application-side of the iPhone." The security hole can also be leveraged to inject Web shell scripts that would give cybercriminals complete control of the affected application directory. If the device is jailbroken, things become even more complicated. On tampered iPhones, an attacker could take control not only of the application folder, but also of the entire phone. Source: http://news.softpedia.com/news/TreasonSMS-Bug-Allows-Hackers-to-Execute-Malicious-Code-on-iPhones-266214.shtml

**Microsoft Office flaw exploited in the wild with malicious documents.** Security researchers from McAfee warn the CVE-2012-0158 vulnerability that exists in Microsoft Office and other products that use MSCOMCTL.OCX is being exploited in the wild with the aid of maliciously crafted RTF, Word, and Excel files. The security hole was patched with the April 2012 updates, but many users failed to apply them, giving cybercriminals the opportunity to launch malicious operations. Experts found the specially designed files come with a vulnerable OLE object embedded, usually being served to users via unsolicited e-mails. When the malevolent file is opened, the victim sees a regular document presented as bait, but in the background, the a trojan is installed. The infection begins when the Word process opens the crafted document. The CVE-2012-0158 flaw is exploited and the shellcode in the OLE file is triggered. This shellcode is responsible for installing the trojan in the Temp folder. At this stage, the same shellcode starts a new Word process and opens the bait document, which is also dropped in the same Temp directory. The first process is terminated and the victim is presented only with the legitimate-looking document. Because in the first step the malicious element is executed and only then the genuine file is run, users whose computers are targeted may see that Word opens, quits, and then, almost immediately, re-launches to display the bait. Source: http://news.softpedia.com/news/Microsoft-Office-Flaw-Exploited-in-Wild-with-Malicious-Documents-266068.shtml

**New Java malware exploits both Windows and Mac users.** Symantec discovered a new form of Java malware that infects Apple and Windows machines. The company's research describes a strain of Java Applet malware that either drops a Python-based malware in Mac operating systems or an executable-form of malware in Windows computers. If opened, both forms could launch a trojan that could trigger a backdoor on the computer, regardless of the platform. The malware exploits the Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability (CVE-2012-0507) to download the malware. The post said the Mac trojan can currently only control polling times, or "how many times it gets commands from the server at certain time intervals." If enabled however, the trojan can also download files, list files and folders, open a remote shell, sleep, or upload files. The trojan for Windows can send information about the infected computer and disk, its memory usage, OS version and user name, in addition to downloading and executing files and opening shells to receive commands.

The news of this malware comes after the discovery of Flashback and SabPub, two forms of malware that targeted Mac users throughout the first quarter of 2012 via another vulnerability in Java. The vulnerability CVE-2012-0507 — an older Java flaw recently blocked by Mozilla's Firefox — was used by some Flashback variants earlier in April, before being patched by Apple. Source: http://threatpost.com/en_us/blogs/new-java-malware-exploits-both-windows-and-mac-users-042412

**FBI, working group reinforce effort to rid computers of DNSChanger.** The FBI and a working group of security experts relaunched their campaign to rid computers of the DNSChanger malware that still threatens to cut hundreds of thousands of users off from the Internet in July. The ad hoc DNSChanger Working Group has a new Web site that links to instructions on how users and organizations can find and remove DNSChanger from their machines, along with updates on the effort. The FBI also has a Web page devoted to fixing the problem. DNSChanger infected as many as 4 million computers around the world as part of an Estonia-based clickjacking scheme the FBI busted in November 2011. The malware redirected infected computers to the ring's servers, which then sent them to bogus sites, while also disabling antivirus software. After the FBI broke up the ring and arrested six of its principals, it received a court order to allow the Internet Systems Consortium to run temporary replacement DNS servers in place of the ring's servers. Otherwise, infected computers would have had their DNS requests sent to servers that were taken offline, effectively cutting them off from the Internet. The original court order was to expire in March, but the FBI obtained an extension until July 9 to allow more time to clean infected machines. Much progress has been made in ridding machines of the malware, and federal agencies have largely been cleaned of infections, but an estimated 350,000 could still be at risk. The new campaign is designed to raise awareness about the threat, so users and organizations check for the malware and remediate the problem if it is on their machines. Source: http://gcn.com/articles/2012/04/24/dnschanger-fbi-working-group-new-campaign.aspx

**Lenovo expands recall of ThinkCentre desktop computers due to fire hazard.** The U.S. Consumer Product Safety Commission, in cooperation with Lenovo, announced a voluntary recall of about 13,000 Lenovo ThinkCentre M70z and M90z computers April 24 (50,500 were previously recalled in March). The manufacturer/importer of the product was Lenovo, of Morrisville, North Carolina. A defect in an internal component in the power supply can overheat and pose a fire hazard. Lenovo received reports of one fire incident and one smoke incident. The computers were sold online at Lenovo's Web sites, by telephone, and direct sales through Lenovo authorized distributors nationwide from May 2010 through March 2012. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12159.html

**100 million users might be affected by a social network vulnerability.** Do-it-yourself social networking company Ning is reportedly suffering from a security problem that could affect 100 million users. Ning lets people set up their own social networking channels. According to a Dutch report, a problem with its security could leave them wide open to account hijackers. A Dutch Web site called Web Wereld said two students exploited cookies to gain log-in control over Ning user accounts. They used a proof-of-concept that showed they could access 90,000 accounts and 100 million users, but had no intention of exploiting it for malicious purposes. They did suggest that if others were able to use it, then they could take over Ning accounts. The students told Ning about the exploit in March, and since then the firm has worked to fix it. Source: http://www.theinquirer.net/inquirer/news/2169403/100-million-users-affected-social-network-vulnerability

**Microsoft yanks Office for Mac 2011 upgrade.** April 20, Microsoft removed a major update for Office for Mac 2011 from its upgrade servers, acknowledging bugs that corrupted the Outlook database on some machines. Office for Mac 2011 Service Pack 2 (SP2) was released April 12. That same day, users who upgraded began reporting problems on Microsoft's support site, saying they were unable to run Outlook, the suite's e-mail client. April 17, Microsoft confirmed the SP2 upgrade could in some cases corrupt the Outlook identity database, and offered workarounds to prevent that from happening for those who did not yet install the service pack, as well as a step-by-step guide to reconstructing the database for those affected by the bug. Three days later, Microsoft took more drastic action, shutting down the delivery of Office for Mac 2011 SP2 through the company's automatic upgrade service. Source: http://www.computerworld.com/s/article/9226445/Microsoft_yanks_Office_for_Mac_2011_upgrade?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google+Reader

**Microsoft yanks Office for Mac 2011 upgrade.** April 20, Microsoft removed a major update for Office for Mac 2011 from its upgrade servers, acknowledging bugs that corrupted the Outlook database on some machines. Office for Mac 2011 Service Pack 2 (SP2) was released April 12. That same day, users who upgraded began reporting problems on Microsoft's support site, saying they were unable to run Outlook, the suite's e-mail client. April 17, Microsoft confirmed the SP2 upgrade could in some cases corrupt the Outlook identity database, and offered workarounds to prevent that from happening for those who did not yet install the service pack, as well as a step-by-step guide to reconstructing the database for those affected by the bug. Three days later, Microsoft took more drastic action, shutting down the delivery of Office for Mac 2011 SP2 through the company's automatic upgrade service. Source: http://www.computerworld.com/s/article/9226445/Microsoft_yanks_Office_for_Mac_2011_upgrade?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google+Reader

## National Monuments and Icons

(Colorado) **Changes recommended to Colorado wildfire response.** State officials recommended organizational changes to the Colorado State Forest Service following a deadly wildfire that grew out of a prescribed burn set by the agency. April 23, the governor announced a proposal to have the agency's wildfire management functions and the state division of emergency management report to the Colorado Department of Public Safety. The state forest service is currently part of Colorado State University (CSU) and reports to academic officials, not state emergency officials. The CSU president said forest research and management would stay under the umbrella of the university. Legislation is needed to enact the change. The governor said the transfer would be smooth and could be accomplished as early as the end of July. Embers from a controlled burn the state forest service set March 22 reignited in heavy winds, sparking a wildfire March 26 near Conifer that damaged at least 23 homes, and left 3 people dead. An April 16 review led by a veteran forest manager examining the controlled burn found firefighters departed from their plan on one point by patrolling the perimeter for only 2 consecutive days after it was ignited. Source: http://www.gazette.com/news/response-137407-wildfire-changes.html

(Utah) **2 arrested for allegedly planting deadly booby traps on Utah walking trail.** Two men were in custody in Utah after deadly booby traps were uncovered along a popular walking trail in Provo Canyon, NewsCore reported April 23. The suspects were charged April 21 with reckless endangerment, a misdemeanor. A statement issued by the Utah County Sheriff's Office said a U.S. Forest Service officer discovered the two booby traps inside a makeshift shelter built from dead tree limbs while on foot patrol along the Big Springs walking trail April 16. "As he investigated the shelter he noticed what appeared to be a trip wire near the ground at an entrance. Upon further investigation he discovered that the trip wire led to a booby trap device which was made with a large rock, sticks sharpened at both ends, and was held together with rope," the statement read. "This device was situated in such a way that when contact was made with the trip wire it would swing toward an unsuspecting hiker or camper," the statement added. A second booby trap was also discovered, also triggered by a trip wire. "This wire was configured so as to trip a person, possibly causing them to fall forward onto sharpened sticks placed in the ground," the statement said. Police said the pair confessed to placing the deadly traps in the makeshift enclosure. Source: http://www.foxnews.com/us/2012/04/23/2-arrested-for-allegedly-planting-deadly-booby-traps-on-utah-walking-trail/

## Postal and Shipping

(Florida) **Mail carrier robbed at gunpoint in Tampa, may have been seeking tax return checks.** The U.S. Postal Service has offered a $50,000 reward for information leading to the arrest of two people who robbed a mail carrier at gunpoint April 25 in Tampa, Florida. Police said a man told the mail carrier to drive to another location. When they arrived, the suspect asked him where the checks were. Authorities believe the robbers were looking for federal income tax returns. The mail carrier was sorting mail in his truck when police said he felt a gun at his side. The Tampa Tribune reported the mail carrier told the suspect the checks might be in a tray. The suspect dumped the contents into a backpack and fled. He was joined at that point by a second man. Source: http://www.foxnews.com/us/2012/04/26/mail-carrier-robbed-at-gunpoint-in-tampa-may-have-been-seeking-tax-return/

## Public Health

(Texas) **Accused serial thief infiltrates dozens of hospitals, clinics in Houston.** Disguised as a nurse wearing scrubs, a serial thief managed to infiltrate dozens of hospitals and clinics around Houston, to steal purses and credit cards. "She's just walking into these hospitals uncontested," said a lieutenant from the Harris County Sheriff's Office. Once inside a hospital or clinic, she "cruises" around to find unmanned purses and then swiftly hits the stores. Investigators linked her to dozens of hospital thefts dating to February 2012. Her latest hit was April 20 at TOPS Specialty Hospital. Wearing scrubs, she slipped in through a back door, but was confronted and questioned by hospital administrators. She convinced them she left her identification in the car, and as she exited, managed to steal another nurse's purse. Authorities asked hospital workers to be on the lookout. Source: http://www.chron.com/news/houston-texas/article/Accused-serial-thief-infiltrates-dozens-of-3503657.php#photo-2851289

**Healthcare industry now sharing attack intelligence.** Large healthcare organizations and the U.S. Department of Health and Human Services (HHS) have banded together to share attack and threat intelligence in a new incident response and coordination effort established specifically for their industry. The Health Information Trust Alliance (HITRUST) announced April 24 the launch of the new HITRUST Cybersecurity Incident Response and Coordination Center as an online community for helping spot cybersecurity attacks against healthcare organizations and coordinating incident response to threats and attacks. According to a founding participant, attacks against healthcare organizations are becoming more targeted and focused, and cyber criminals are going after Web portals and healthcare applications as their point of entry, rather than the previous method of hitting the perimeter. Source: http://www.darkreading.com/database-security/167901020/security/attacks-breaches/232900882

**WMD treatment development poses significant challenges, GAO says.** There are many obstacles to development of medical countermeasures that can be used to treat victims of a weapons of mass destruction (WMD) attack, including the high rate of failure in efforts to put treatments on the market, the U.S. Government Accountability Office (GAO) said in a report issued the week of April 16. There are "few" accessible vaccines and other drugs that could be used to aid people exposed to chemical, biological, radiological, or nuclear agent, the study said. "The failure rate for development and licensure of most drugs, vaccines, and diagnostic devices can be more than 80 percent, depending on the stage of scientific research and development," the agency said. "Given this risk, as well as a lack of a commercial market for most medical countermeasures, attracting large, experienced pharmaceutical firms to research and develop them is challenging." The GAO report also noted the need to ensure the effectiveness of treatments without actually exposing humans to WMD agents in testing; difficulties in establishing the correct dosage for children; and assessing the "safety and effectiveness" of unlicensed drugs that might be authorized for use during a health crisis. "Finally, HHS faces the logistical challenge of ongoing replenishment of expiring medical countermeasures in the U.S. Strategic National Stockpile, the national repository of medications, medical supplies, and equipment for public health emergencies," according to

GAO findings. Source: http://www.nti.org/gsn/article/wmd-treatment-development-poses-significant-challenges-gao-says/

## Transportation

**U.S. aging bridges in critical condition.** There are an estimated 18,000 bridges in the United States which are classed as fracture-critical bridges, requiring continual inspections, Homeland Security News Wire reported April 23. The need for increased inspection and maintenance runs against shrinking state and federal budgets for infrastructure improvements. The American Society of Civil Engineers' (ASCE) most recent report card gave the condition of bridges in the U.S. a grade of C. The ASCE notes 26 percent of U.S. bridges are either structurally deficient or functionally obsolete. They note that as of 2008, the year of the most recent pre-report card survey, one in four bridges in rural areas was deficient, while one in three urban-area bridges are in the same class. Under ASCE definition, structurally deficient bridges, though not unsafe, must post speed and weight restrictions because of limited structural capacity. A functionally obsolete bridge, though not unsafe either, has older design features and geometrics, and cannot accommodate current traffic volumes, vehicle sizes, and weights. Source: http://www.homelandsecuritynewswire.com/dr20120423-u-s-aging-bridges-in-critical-condition

## Water and Dams

(Georgia) **Another bomb found at the dam.** Georgia Bureau of Investigations (GBI) agents were working to figure out who left a bomb at the Georgia Power Dam in Albany, Georgia, April 26. Dougherty County police reported the explosive was found at the bottom of the boat ramp and called the GBI Bomb Squad to diffuse it. This is the second explosive found at the dam in recent weeks. Earlier this month, a man was arrested for having explosives near the dam. Source: http://www.walb.com/story/17835068/this-is-the-second-time-in-weeks-a-bomb-was-found-at-the-dam

## North Dakota Homeland Security Contacts

**To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.**

**To contribute to this summary or if you have questions or comments, please contact:**

**Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168**